


09/700,160
P.F.D. 12/14/00
Simon Qin
20/3

What is claimed is:

Pub B1 
1. A backup/recovery system for protecting a computer system, said backup/recovery system is installed in said
5 computer system, said computer system including an application layer, said application layer coupled to an interface and operating predetermined application programs, said backup/recovery system BEING CHARACTERIZED BY

10 - a detecting module, located within said computer system, for monitoring a predetermined message;

Wherein said detecting module retrieves said predetermined message, in order to determine whether there is a predetermined harmful data contained therein for judging said backup/recovery system to backup data or not,
15 said interface implements a predetermined procedure thereafter and said application layer involves reading said predetermined message.

2. The system of claim 1 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communications
5 link.

3. The system of claim 2 wherein said network device is coupled to a server device.

4. The system of claim 3 wherein said server device is capable of controlling said client device's backup/recovery conduct remotely and immediately.

pub. B1

5 5. The system of claim 2 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

5 6. The system of claim 2 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

5 7. The system of claim 1 wherein said predetermined harmful data comprises a file in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP form.

5 8. A method for protecting a computer system, said method comprising:

- 5 - Retrieving a predetermined message to be downloaded to said computer system;
- Determining whether there being a predetermined harmful data contained in said predetermined message; and;
- 10 - Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined message.

5 9. The method of claim 8 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communications link.

Pub B1

10. The method of claim 9 wherein said network device is coupled to a server device.

11. The method of claim 10 wherein said server device is capable of controlling said client device's backup/recovery conduct remotely and immediately.

12. The method of claim 9 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

13. The method of claim 9 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, RPC, HTTP, and IIOP.

14. The method of claim 8 wherein said predetermined harmful data comprises a file in a predetermined form, comprising one or more of the group consisting of *.EXE, *.DOC, and *.ZIP form.

15. A method for protecting a computer system with a backup/recovery system, said computer system including an application layer, said application layer coupled to an interface and operating predetermined application programs, said method comprising:

- Installing said backup/recovery system in said computer system, said backup/recovery system having a detecting module for monitoring a predetermined message located within said computer system;

pub B1

15

20

- Retrieving said predetermined message to be downloaded to said computer system;
- Determining whether there being a predetermined harmful data contained in said predetermined message;
- Backing up data stored in said computer system at the time said predetermined harmful data being contained in said predetermined message;
- Implementing a predetermined procedure by said interface; and
- Indicating said application layer read said predetermined message.

5

16. The method of claim 15 wherein said backup/recovery system is coupled to a network device, said network device is coupled to at least one client device by a communications link.

17. The method of claim 16 wherein said network device is coupled to a server device.

18. The method of claim 17 wherein said server device is capable of controlling said client device's backup/recovery conduct remotely and immediately.

5

19. The method of claim 16 wherein said network device comprises a network means, comprising one or more of the group consisting of a LAN, WAN, Internet, Intranet, Extranet and wireless network.

Pub 31

20. The method of claim 16 wherein said network device comprises a communication means, comprising one or more of the group consisting of electronic mail, TCP/IP sockets, 5 RPC, HTTP, and IIOP.